Hackeando los ciber-riesgos en la cadena de suministro: Para entender los controles correctos, hay que mirar el sistema

Sepúlveda Estay, Daniel Alberto; Khan, Omera

Published in:
Logistec

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

THEWORLDNEWS II

HACKEANDO LOS CIBER-RIESGOS EN LA CADENA DE SUMINISTRO: PARA ENTENDER LOS CONTROLES CORRECTOS, HAY QUE MIRAR EL SISTEMA

Publicado en Martes, 05 Enero 2016 18:44 | Impactos: 444

Si se consideran tanto la creciente complejidad de las redes de abastecimiento, como la consecuente exposición de estas redes a interrupciones inesperadas ocasionadas por ciber-ataques, se requiere una forma más amplia para entender los ciber-riesgos en las cadenas de suministro. En este artículo se describen algunas de las razones por las que los métodos de evaluación de riesgos actuales son insuficientes, se proporciona una analogía para entender los efectos dinámicos en una empresa, se describe en términos generales lo que significa entender los ciber-riesgos desde el punto de vista de teoría de control, y se enuncia una nueva forma de entender la resiliencia en la cadena de suministro. Nuestro trabajo propone un cambio foco desde la confiabilidad de los componentes individuales en la cadena de suministro, hacia el control y un entendimiento más profundo del sistema.

EL DESAFÍO DE LAS CADENAS DE SUMINISTRO ACTUALES

Las complejas cadenas de suministro que estamos construyendo están creando nuevas vulnerabilidades en estos sistemas, exponiendo las organizaciones a nuevos riesgos. Muchos de estos riesgos son originados por la creciente dependencia de las cadenas de suministro competitivas en las tecnologías de la información (IT). Las organizaciones bajo ataque están siendo perjudicadas por ejemplo a través de interrupciones a sus operaciones, o por la pérdida de datos de la empresa y/o propiedad intelectual, con la consiguiente pérdida en el valor a la organización. Estudios han demostrado costos anuales potenciales de más de 550 mil millones de dólares a causa de estos riesgos. Estos trastornos están poniendo a prueba la manera en que organizamos nuestras actividades operativas, así como la manera en que manejamos las relaciones con nuestros socios. Esto también ha dejado en evidencia que el acceso transparente y rápido a los recursos que el IT ha facilitado en la cadena de suministro, es la misma plataforma utilizada por hackers para su propio beneficio.

La variedad de potenciales interrupciones ha dejado además en evidencia que las herramientas tradicionales de evaluación de riesgos siendo utilizadas son poco prácticas para riesgos emergentes o que evolucionan rápidamente. Las empresas muchas veces no tienen los recursos para analizar cada potencial modo de falla, o para actualizar estas evaluaciones a medida que aparecen nuevos riesgos, o los riesgos conocidos cambian.

Nuestra investigación en la Universidad Técnica de Dinamarca (DTU) nos está llevando a cuestionar la idoneidad del análisis de riesgos tradicional utilizado en las cadenas de suministro complejas. Hemos encontrado que se pueden lograr mejoras al pasar de un análisis estático, basado en el análisis de confiabilidad de los componentes individuales, a un análisis dinámico, basado en el control de las vulnerabilidades de la organización, como lo resume la Figura 1.

Figura 1 – Cambio de análisis propuesto

ANÁLISIS TRADICIONALES DE CIBER-RIESGOS TIENEN DEFICIENCIAS

La Administración Federal de Aviación en los EE.UU. recientemente ha identificado más de cien métodos para evaluar riesgos varios de los cuales se utilizan tradicionalmente para la evaluación de riesgos en cadenas de suministro. Estos métodos se basan en gran medida en el supuesto de que un evento indeseable es causado por una cadena de otros eventos precedentes 2. Estos análisis identifican este evento indeseable y razonan hacia atrás, identificando acontecimientos que condujeron a este evento final, hasta que se identifica el evento que es considerado el creador de la cadena, la llamada "causa raíz". Tal es el caso de los métodos tales como Análisis de Modos de Falla y Efectos (o sus siglas en ingles FMEA - Failure Mode and Effect Analisis) o Análisis de Modo de Falla y de Criticidad (o sus siglas en inglés FMECA Failure Mode and Criticality Analysis). Estos son denominados como análisis "retrospectivos". Si por el contrario se

hace un análisis para revelar todas las posibles cadenas de eventos en los que algo puede salir mal, se utilizan métodos como el "Análisis de árbol de falla" (o sus siglas en ingles FTA, Failure Tree Analysis). Estos son conocidos como métodos de análisis "prospectivos". Varios otros métodos prospectivos también se utilizan ampliamente, como el Análisis de Peligros y Operabilidad (HAZOP, Hazard and Operability Analysis) o el Análisis de Árbol de Eventos (ETA, Event Tree Analysis).

Todos estos métodos siguen el modelo de causalidad basado en "cadena de fallas", que puede ser mejor representado a través de la analogía de una fila de fichas de dominó cayendo. Hay un dominó inicial, etiquetado la "causa raíz", que representa un único evento. Puede ser un error humano o un fallo de un componente. Este error se propaga a través del sistema, dando lugar a otros fallos de los componentes y que resulta finalmente la caída del último dominó, equivalente a experimenta el problema síntoma que es el ciber-ataque, como representado en la Figura 2.

Figura 2 - Representación de la cadena de fallas como domino

Esta "familia" de los métodos ha sido ampliamente utilizada desde su invención en la década de 1950. Son muy populares debido a su relativa simplicidad, además de su eficacia en el análisis de sistemas con componentes técnicos, así como en sistemas simples que involucren tanto a personas (operarios) como a componentes técnicos, los llamados "sistemas socio-técnicos". Una forma tradicional de la cuantificación de los ciber-riesgos sería identificar todas las formas en una cadena de suministro podría fallar (análisis de confiabilidad), o ser objeto de ciber-ataque. Esto se hace normalmente en estrecha interacción con un equipo con experiencia de diferentes áreas de la cadena de suministro bajo análisis. El equipo entonces se pone de acuerdo sobre la probabilidad de ocurrencia de cada uno de estos posibles modos de falla (probabilidad), y una cantidad aproximada de dinero equivalente a la perdida en caso de que estas fallas se produjeran (Severidad). Impacto sería entonces Probabilidad multiplicado por la Severidad para cada una de estas fallas. Así se obtiene una clasificación y jerarquización de las fallas, permitiendo la identificación de los eventos con mayor impacto. Además las acciones se pueden concentrar esfuerzos en la eliminación o mitigación de los riesgos más importantes.

Nuestra investigación en la Universidad Técnica de Dinamarca nos está llevando a cuestionar varios de los supuestos acerca de cómo nuevos riesgos tales como los ciber-riesgos pueden ser manejados, y dada la aparición creciente de diferentes tipos de ciber-ataques con efectos potencialmente dañinos en el rendimiento de la cadena de suministro. Como resultado, nos encontramos en la búsqueda de formas alternativas para entender estos riesgos, y esto nos esta llevado a la generación de propuestas prácticas específicas para su manejo.

La forma tradicional de la cuantificar riesgos presenta varias deficiencias. Analizaremos cuatro de ellas: la confiabilidad versus seguridad, la subjetividad de elección, los efectos sistémicos, y el comportamiento dinámico.

CONFIABILIDAD VERSUS SEGURIDAD

Al centrarse únicamente en el rendimiento de las partes individuales de la cadena de suministro, existe el peligro de erróneamente interpretar confiabilidad como seguridad, dado que en general se supone que si los componentes de la red de abastecimiento funcionan bien (son confiables), entonces esta red de abastecimiento es segura, lo que no es necesariamente cierto. Esta creencia se desmorona cuando se producen errores en las redes de suministro donde todos los componentes funcionan como se esperaba, incluso a veces porque todos los componentes funcionaron como se esperaba. Esto puede ocurrir especialmente cuando se ha integrado algún tipo de redundancia al sistema, o cuando los controladores (humanos o automáticos) no entienden adecuadamente lo que realmente sucede en el proceso. La redundancia puede funcionar bien en sistemas mecánicos o eléctricos simples, pero cuando se aplica a las redes de decisión, puede dar lugar por ejemplo a una llamada doble, en el que dos personas diferentes a tomar decisiones contradictorias, un problema potencial importante en situaciones en las que es necesaria una acción urgente. Además, en caso de que las acciones de control en los procedimientos no representan lo que debe ser hecho, si este procedimiento de control que funciona correctamente, podría dar lugar a una interrupción no deseada.

LA CAUSA RAÍZ DEPENDE DE QUIÉN ESTÁ REALIZANDO EL ANÁLISIS

En los métodos tradicionales de evaluación de riesgos, hay una selección subjetiva de la cadena de acontecimientos. La lista de posibles fallos, la cadena de acontecimientos que conducen a este fallo, así como las relaciones entre los eventos de la cadena hasta llegar a la "causa raíz", son altamente dependientes de quién está haciendo el análisis. Esto puede dar lugar a varios tipos de sesgos. Si los participantes están en puestos de dirección (management), sin un conocimiento profundo de las operaciones, algunas fuentes operacionales relevantes para fallos van a estar ausentes de la lista. Potencialmente las “causas raíz” podrían ser seleccionados sólo porque son políticamente aceptables, a la vez que otras explicaciones potenciales para la falla no son exploradas, ya que pueden ser fuente de vergüenza para la organización. Otro aspecto importante es que muchas veces esta búsqueda causal termina con algún tipo de "error del operador" o "falta de formación". Jens Rasmussen, un conocido investigador de Risø (actual DTU) mencionaba ya en la década de 1980 que

de hecho es muy difícil de analizar "a través" de un error humano, y por lo tanto el análisis se detiene allí.

EFECTOS SISTÉMICOS: AMPLIAR LA MIRADA

Los métodos tradicionales sólo toman en cuenta una cadena muy limitada de eventos, excluyendo factores que no estén directamente incluidos en una cadena causal de acontecimientos. Esto implica que la explicación generalmente considera los eventos que conducen inmediatamente a la pérdida, y los factores sistémicos no son considerados. Factores sistémicos pueden ser las consecuencias que una decisión tiene en otras partes de la organización, y que eventualmente afectan y se contraponen a la decisión original a través de circuitos organizacionales de retroalimentación. Esto normalmente no ocurre inmediatamente. (Ver Figura 3). Los efectos sistémicos pueden incluir aspectos tales como decisiones de política de empresa, que generan condiciones operacionales que llevan a interrupciones no deseadas.

Figura 3 -Peligros de no considerar las retroalimentaciones organizacionales

Los métodos tradicionales dificultan una adecuada comprensión de la conducta organizacional deseada y la capacidad de soportar las interrupciones de los ciber-ataques para recuperar las condiciones normales de funcionamiento (cyber-resiliencia). La reacción de la empresa, al tener que hacer frente a un ciber-ataque, normalmente será una serie de acciones utilizando los recursos existentes en la empresa. Estas acciones se desarrollan con el tiempo, y con el tiempo también se restaura la estabilidad de la operación. Esto no va a suceder de inmediato, lo que significa que los ciber-resiliencia es en realidad un comportamiento dinámico de la cadena de suministro, y como tal, requiere una forma de entender esta dinámica. Veamos esto en más detalle.

DINÁMICA: NEGOCIOS VERSUS AUTOMÓVILES

Los efectos dinámicos pueden entenderse mejor mediante la comparación de una empresa de fabricación sujeta a ciber-ataques, con un automóvil en la carretera. El gerente de una empresa sería equivalente al conductor del automóvil. Ciber-riesgos que vienen hacia esta empresa se pueden representar como obstáculos en la carretera que vienen hacia el automóvil. Este automóvil tiene varios controles que pueden ser utilizados por el conductor para evitar estos obstáculos, tales como el volante, el acelerador y los frenos para nombrar unos pocos. De la misma manera, la compañía tiene también algunos controles que pueden ser utilizados por su gerente para “dirigir” el desarrollo de la empresa, tales como la definición de objetivos estratégicos, la inversión en formación, o de las estructuras de incentivos hacia la colaboración con los proveedores, para nombrar unos pocos.

El automóvil tiene una masa que se traduce en "efectos inerciales". No es posible o conveniente para el conductor para cambiar la dirección del automóvil repentinamente, o acelerar o detener el automóvil de repente debido al riesgo de un accidente por efecto de la masa del automóvil. Los efectos inerciales son una de las características de los sistemas reales, conocidos como "efectos dinámicos". Una empresa también tiene "efectos inerciales", tales como el número de empleados, las cuentas por pagar el total o el número de pedidos electrónicos para los productos. Esto significa que un gerente no puede hacer cambios repentinos en los controles organizacionales, por ejemplo en el caso del riesgo de un ciber-ataque, sin consecuencias a raíz de los “efectos inerciales” presentes en la organización.

Un conductor evita un obstáculo en el camino mediante el uso de los controles disponibles, por ejemplo, mediante la activación de los frenos en una señal próxima de “Pare”. Un conductor con poca experiencia relevante tal vez intentará frenar demasiado tarde, los que nos empujará hacia adelante con una sacudida. Un recordatorio no siempre-suave del efecto inercial de nuestras propias masas en movimiento. De la misma forma, en el caso de la empresa, un gerente tratando de evitar los efectos de un ciber-ataque utilizará los controles a su disposición. Un gerente con poca experiencia relevante tal vez intente cambiar los objetivos estratégicos con demasiada rapidez o cambiar las estructuras de incentivos radicalmente, creando así una "sacudida" de la organización.

MUCHOS EFECTOS INERCIALES SON DESCONOCIDOS PARA LOS GERENTES

Algunas importantes diferencias salen a la luz con esta analogía, las que hemos definido como diferencias de "gestión" y diferencias de "diseño". Los conductores normalmente comienzan conducción ("gestión") del automóvil desde una posición de reposo, y con entrenamiento, el conductor explorará gradualmente crecientes niveles de dificultad para conducir. En el caso de la empresa, el gerente general será nombrado para el papel con la compañía ya "en el movimiento" a una velocidad indeterminada. El gerente a su vez tendrá una serie de controles. Algunos de ellos serán familiares para él a raíz de su experiencia previa, y algunos podrían ser nuevos controles, implementados por su predecesor. Hay diferentes "masas" de la organización que el gerente no necesariamente conoce, y tendrán que descubrir por ensayo y error. Por otra parte, el gerente no tendrá experiencia en los efectos en la inercia organizacional que estos controles a su disposición

tendrán en la empresa. Por último, en la misma forma que se enseñan a conducir un automóvil en la escuela de conducción por medio de exponer a los alumnos a los distintos automóviles actuales y las potenciales condiciones de conducción, los gerentes son “entrenados” en las escuelas de negocios sobre las empresas existentes y las potenciales condiciones de negocio. Todas estas diferencias son diferencias de “gestión”.

Otras diferencias importantes y muy relevantes son las de diseño. Un automóvil tiene una estructura, desarrollada y mejorada con el tiempo por un equipo de especialistas. Ellos entienden los efectos que esta estructura tiene sobre el comportamiento del vehículo, con especial atención en los efectos dinámicos. Sin embargo y por otro lado, la estructura de una empresa no suele haber sido diseñada, sino más bien replicada de otros modelos organizacionales en funcionamiento, y con posterior crecimiento organizacional a través de la adquisición de otras empresas (crecimiento inorgánico) o a través de su propia expansión (crecimiento orgánico). Las estructuras empresariales son por lo tanto muy propensas a ser desarrolladas sin consideraciones dinámicas en su diseño.

LOS RIESGOS COMO UN PROBLEMA DE CONTROL

Tomando la analogía del automóvil un paso más allá, la resiliencia, esto es la capacidad de recuperación y de devolver las operaciones a niveles normales después de alguna interrupción, puede entonces entenderse como la capacidad de la empresa para ajustar el curso de sus procesos mediante el uso de sus estructuras de control. Esto se puede representar de manera simplificada de acuerdo a la Figura 4.

Figura 4 – representación de un proceso de control

La resiliencia se refleja entonces en lo bien que funciona la estructura de control a través de:

Lo efectivo y oportuno de los "sensores" que miden el proceso actual • lo efectivo y oportuno de nuestra intervención en el proceso por medio de los "actuadores" existentes cuando hay algo que debe ser hecho, y • lo efectivo y oportuno de la traducción en nuestra cadena de suministro por medio de su ”controlador” y que transforma lo indicado por los “sensores” organizacionales en acciones específicas a ser ejecutadas por los “actuadores”.

Esta es una actividad continua, ya que el proceso de suministro está constantemente encontrando diferentes condiciones de trabajo que tienen que ser detectadas, analizadas, y a las cuales las organizaciones se debe adaptar.

Pasos para implementar ciber-resiliencia con un enfoque de control: La ciber-resiliencia en la cadena de suministro desde el punto de vista de control pueden ser alcanzada por medio los siguientes pasos generales, y que deben ser realizadas por un equipo de la empresa bajo la orientación y guía de expertos en este tipo de análisis:

Identificar lo que la empresa considerará como interrupciones indeseables a la cadena de suministro (identificar posibles accidentes) • Identificar la combinación de las condiciones de la red de suministro que llevarían a las interrupciones no deseadas especificadas en el paso anterior (Identificar los peligros), • Definir los límites de lo que está en el control, como también fuera del control de la empresa (Identificar los límites del sistema de alimentación, controles y "masas" presentes en el sistema) • Realizar una lluvia de ideas sobre cómo podría ocurrir cada interrupción potencial, identificada en el primer paso. Esto dará lugar a la identificación de mejoras potenciales en los controles existentes, o la necesidad de nuevos controles, o de otros controles que debe estar en lugar de controles existentes.

Acerca de los Autores

Omera Khan, PhD., es profesor de Dirección y gestión de Operaciones de la Universidad Técnica de Dinamarca. Ella trabaja con organizaciones líderes en una variedad de problemas de la cadena de suministro y logística, y es asesor de muchas universidades en desarrollo cursos de logística, cadenas de suministro y gestión de operaciones. Ha dirigido y llevado a cabo proyectos de investigación encargados por agencias gubernamentales, consejos de investigación y empresas en la capacidad de recuperación de la cadena de suministro, la capacidad de respuesta, la sostenibilidad e impacto del diseño de productos en la cadena de suministro. Su área más reciente de investigación se centra en los ciber-riesgos y la capacidad de recuperación de la cadena de suministro. Omera es asesor de muchas organizaciones y ofrece consultoría especializada en la gestión de riesgo de la cadena de suministro. Ella es una presentadora muy aclamada y es invitada regularmente como orador principal en conferencias mundiales y eventos corporativos. Ha publicado su investigación en las principales revistas, ha contribuido a varios capítulos de libros, y es el autor principal del libro “Handbook for Supply Chain Risk Management: Case Studies, Effective Practices and Emerging Trends”. También ha sido profesor visitante en varias escuelas de negocios.

Daniel A. Sepúlveda Estay, MSc., es un investigador de doctorado (PhD) en la Universidad Técnica de Dinamarca, donde investiga el tema de “ciber-riesgo y seguridad en la cadena de suministro global”. Ha trabajado en las divisiones de ingeniería y suministro de una serie de empresas multinacionales, tanto en posiciones estratégicas y de liderazgo, como en roles operacionales por más de 11 años, participando en iniciativas tales como la implementación de excelencia operacional incluyendo lean manufacturing en plantas de Coca-Cola Company en América Latina y la racionalización de suministro en proyectos de la división Copper en BHP Billiton. Daniel es Ingeniero Civil Mecánico de la Universidad Técnica Federico Santa María en Valparaíso, Chile, con un grado de Magister en Ingeniería Industrial de la Pontificia Universidad Católica de Chile en Santiago, Chile, y un grado de MSc., en Management de la Sloan School of Management del Massachusetts Institute of Technology , en Boston, Estados Unidos.

Autores : Daniel Sepúlveda, MSc., Investigador de PhD, DTU Management Engineering, DTU Universidad Técnica de Dinamarca, dasep@dtu.dk" data-mce-href="mailto: dasep@dtu.dk" style="line-height: 19.8px;"> dasep@dtu.dk . Omera Khan, PhD., Profesor de Gestión de Operaciones, of Operations Management, DTU Universidad Técnica de Dinamarca, okhan@dtu.dk" data-mce-href="mailto: okhan@dtu.dk" style="line-height: 19.8px;"> okhan@dtu.dk

---